IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

MATTHEW CRABTREE and BETTY ROBINSON-HARRIS, *individually, and on behalf of all others similarly situated*, *Plaintiffs*, v. MARRIOTT INTERNATIONAL, INC., *Defendant*.	CASE NO: COMPLAINT (CLASS ACTION) **JURY TRIAL DEMANDED**

1. On November 30, 2018, Marriott International, Inc. ("Marriott" or "Defendant"), the parent of Starwood Hotels & Resorts Worldwide, LLC ("Starwood"), admitted that it had unknowingly allowed hackers to perpetrate the theft of the highly sensitive personal information of over 500 million of its customers. Marriott could have prevented this theft if it had employed reasonable, industry-standard security measures. Marriott's cybersecurity efforts were so deficient that hackers accessed its systems undetected for more than four years[1] during which Marriott failed to encrypt certain of the sensitive personal information it requested from its guests.

2. Plaintiffs bring this class action because Marriott failed to secure and safeguard personally identifiable information ("PII"), such as Plaintiffs' and Class Members' names, mailing addresses, phone numbers, email addresses, passport numbers, account information, date

[1] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WSJ, Dec. 2, 2018, https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

of birth, gender, and other personal information, as well as credit and debit card numbers and other payment card data ("PCD").

3. Marriott admits that hackers appear to have accessed some combination of name, mailing address, phone number, email address, passport number, account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences for 327 million guests, as well as more limited personal information for approximately 170 million additional guests.[2] Marriott, as of this filing, is unable to rule out the possibility that the information necessary to decrypt payment card numbers was also taken.[3]

4. Marriott allowed thieves to access extremely comprehensive information about its guests, placing all of them at a high risk for particularly damaging identity theft.[4] Marriott's actions here are and have been unreasonable: as Senator Edward J. Markey stated, "[c]hecking in to a hotel should not mean checking out of privacy and security protections."[5] Yet, as one privacy expert explained, "[i]t's astonishing how long it took [Marriott] to discover they were breached. For four years, data was being pilfered out of the company and they didn't notice.

---

[2] Starwood Guest Reservation Database Security Incident, Nov. 30, 2018 https://answers.kroll.com/ (last accessed Dec. 7, 2018); *see also* Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, W.S.J., Dec. 2, 2018, https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659 ("For about 327 million customers, the hackers may have gained access to passport numbers, travel details and, in some cases, credit-card information, as well as names and addresses, it said. Investigators also found a file of about 170 million customers created by the hackers that contains much less information, the company said Sunday.").

[3] *Id.*

[4] Taylor Tedford, *Schumer: Marriott should pay for new passports compromised by data* breach, WASH. POST, Dec. 3, 2018, https://www.washingtonpost.com/business/2018/12/03/schumer-marriott-should-pay-new-passports-compromised-by-data-breach/?utm_term=.b147e6c84724 ("The experts will tell you, there is an art to identity theft and it lies in the ability to paint the most complete picture of the person whose information you're looking to steal or sell," Schumer said. "Unfortunately, for many travelers who have stayed in one of Marriott's Starwood hotels, they've provided the company with an array of personal color — like their passport information — that thieves can now access to complete the canvass and assume or sell an identity.").

[5] *Id*.

They can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing."[6]

5. Marriott's intentional, willful, reckless, and/or negligent conduct—failing to prevent the hack, failing to limit its severity, and failing to detect it in a timely fashion—damaged Plaintiffs and all of the Class Members uniformly. For this reason, Marriott should pay for new passports, appropriate identity theft protection, and reimburse its customers the money they would not have paid Marriott had it disclosed its substandard security practices. Plaintiffs' PII and PCD remains stored in Marriott's computer systems. Plaintiffs and Class Members are therefore entitled to injunctive and other equitable relief that safeguards their information, requires Marriott to significantly improve its security, and provides independent, expert oversight of Marriott's security systems.

PARTIES

Plaintiff Matthew Crabtree

6. Plaintiff Matthew Crabtree is a citizen and resident of Colorado.

7. Mr. Crabtree was a guest in numerous Marriott hotels during the Class Period.[7]

8. Mr. Crabtree provided his PII and PCD to Marriott, including his passport information, with the reasonable expectation that it would keep this sensitive information of his secure, and that Marriott would promptly notify him in the event of any breach. Marriott failed in all respects and Mr. Crabtree suffered damages due to the breach.

Plaintiff Betty Robinson-Harris

9. Plaintiff Robinson-Harris is a citizen and resident of California.

---

[6] Nicole Perlroth, et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES, Nov. 30, 2018, https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

[7] As set forth in the definition of the Class, *infra*, the Class Period is January 1, 2014 through September 10, 2018.

10. Ms. Robinson-Harris was a guest in Marriott hotels during the Class Period.

11. Ms. Robinson-Harris provided her PII and PCD to Marriott with the reasonable expectation that it would keep this sensitive information of hers secure, and that Marriott would promptly notify her in the event of any breach. Marriott failed in all respects and Ms. Robinson-Harris suffered damages due to the breach.

Defendant Marriott International, Inc.

12. Marriott is a Delaware Corporation with a principle place of business in Bethesda, Maryland. In 2016, Marriott acquired Starwood. A single, massive database that contains information about approximately 500 million guests (the "Reservation Database") for eleven Starwood hotel brands was the subject of the breach. These hotel brands are: the W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels (collectively referred to as the "Starwood Properties").

JURISDICTION AND VENUE

13. Subject matter jurisdiction is proper because this case has been brought as a class action, the aggregate claims of the Class exceeds $5 million exclusive of interest and costs, the Class includes more than 100 members, and one or more of the members of the Class resides in a state that is different from the state in which Marriott resides. *See* 28 U.S.C. § 1332(d)(2)(A & C).

14. Personal jurisdiction is proper over Marriott because it resides in this District and regularly conducts business here. Upon information and belief, a substantial portion of the events and conduct giving rise to this litigation occurred in this District.

15. Venue is proper because at least one Marriott hotel is located in and transacts business in this district, a substantial portion of the events and conduct giving rise to the

litigation violations complained of in this action occurred in this district, and a substantial portion of the injury from Marriott's conduct occurred in this district. Because Marriott's headquarters are in this District, efficiencies can be gained by litigating this case here, as documents and evidence—including individuals who may be able to provide deposition testimony—are located within this District. *See* 28 U.S.C. §1391(b)(1&2).

CHOICE OF LAW

16. Pursuant to the law of the State of Maryland, including its choice-of-law principals, Maryland state law applies to the claims of Plaintiffs and the Class. In the alternative, Plaintiffs, who reside in the States of Colorado and California, brings claims under Colorado and California state law.[8]

ADDITIONAL FACTUAL ALLEGATIONS

A. Marriott collects customers' PII and PCD.

17. In September 2016, Marriott acquired the assets and liabilities of Starwood for $13.6 billion. Through that acquisition, Marriott came to control the rights to the Starwood Properties.

18. In total, the Marriott hotel chain runs more than 6,700 properties around the world.

19. In order to stay at one of the Starwood Properties, a prospective guest must provide a significant amount of PII such as her name, passport, and address. She also must provide PCD, including debit and credit card numbers. Marriott generally does not destroy this information; rather, it typically stores that information in its Reservation Database.[9]

---

[8] Colorado's consumer fraud statute is substantively similar to the laws of Connecticut, Delaware, Florida, Illinois, Massachusetts, Minnesota, New Jersey, New York, and Washington. *See Yarger v. ING Bank, fsb*, 285 F.R.D. 308, 323 (D. Del. 2012).

[9] Starwood Guest Reservation Database Security Incident, Nov. 30, 2018, https://answers.kroll.com/ (last accessed Dec. 7, 2018); *see also* Robert McMillan, *Marriott's*

20. Marriott has admitted that the information in the Reservation Database includes at least some combination of name, mailing address, phone number, email address, passport number, account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences for 327 million guests, as well as payment card information for additional guests.[10]

21. On September 8, 2018, Marriott learned that someone (or some group) was attempting to access the Reservation Database.[11] When Marriott investigated further, it learned that hackers had first gained unauthorized access to the Reservation Database in 2014, and that these hackers had copied and encrypted information, as well as at least attempted to remove (or "exfiltrate") it.[12]

22. Investigators of the hack have commented that "multiple hacking groups may have simultaneously been inside Starwood's computer networks since 2014."[13] The ability for multiple hackers to simultaneously breach Marriott demonstrates the company's failure to adequately safeguard information.

Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say, WSJ, Dec. 2, 2018, https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659 (last accessed Dec. 7, 2018) ("For about 327 million customers, the hackers may have gained access to passport numbers, travel details and, in some cases, credit-card information, as well as names and addresses, it said. Investigators also found a file of about 170 million customers created by the hackers that contains much less information, the company said Sunday.").

[10] *Marriott says its Starwood database was hacked for approximately 500 million guests*, CNBC, Nov. 30, 2018, https://www.cnbc.com/2018/11/30/marriott-says-its-starwood-database-was-breached-onapproximately-500-million-guests-.html (last accessed Dec. 7, 2018).

[11] Starwood Guest Reservation Database Security Incident, Nov. 30, 2018, https://answers.kroll.com/.

[12] *Id.*

[13] *Clues in Marriott hack are said to implicate China*, Reuters, Dec. 5, 2018, https://www.cnbc.com/2018/12/06/clues-in-marriott-hack-are-said-to-implicate-china.html (last accessed Dec. 7, 2018).

B. In Its Global Privacy Statement Marriott promises to maintain adequate data and cyber security.

23. Marriott publishes a detailed "Global Privacy Statement" which it purports governs its relationships with its customers.[14] Marriott proclaims that customers, by using Marriott's website, its applications, its social media pages, or its offline channels (such as reserving a room in person or over the phone), "agree to the terms and conditions of this [Global] Privacy Statement."[15]

24. Marriott's Global Privacy Statement describes the breadth of personal information that it collects from its customers. In particular, Marriott acknowledges that:

> [a]t touchpoints throughout your guest journey, we collect Personal Data in accordance with law, such as:
>
> - Name
> - Gender
> - Postal address
> - Telephone number
> - Email address
> - Credit and debit card number or other payment data
> - Financial information in limited circumstances
> - Language preference
> - Date and place of birth
> - Nationality, passport, visa or other government-issued identification data
> - Important dates, such as birthdays, anniversaries and special occasions
> - Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
> - Employer details
> - Travel itinerary, tour group or activity data
> - Prior guest stays or interactions, goods and services purchased, special service and amenity requests
> - Geolocation information
> - Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

[14] Marriott Group Global Privacy Statement, Last Updated: May 18, 2018, https://www.marriott.com/about/privacy.mi (last accessed Dec. 7, 2018).
[15] *Id.*

In more limited circumstances, we also may collect:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences and personalized data ("Personal Preferences"), such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit[16]

25. In all respects, the Global Privacy Statement indicates that Marriott will safeguard and limit the disclosure of customers' PII and PCD.

26. *First*, it gives the misleading impression that Marriott uses "reasonable organizational, technical and administrative measures to protect Personal Data."[17]

27. *Second*, the Global Privacy Statement limits the uses to which data can be sent in a section titled "Disclosure of Personal Data and Other Data."

28. *Third*, the Global Privacy Statement provides measures, such as identity verification, to protect customers' PII and PCD. Should a customer request to "access, change,

[16] *Id.*

[17] *Id.*; Marriott's Privacy Policies dating back to 2014 contain similar language about safeguarding personal information. *See* Global Privacy Statement, United States and Canada, Updated Feb. 13, 2014, https://web.archive.org/web/20150202072830/http:/www.marriott.com/marriott/privacy-us.mi, last accessed Dec. 7, 2018 ("Security of Personal Information[.] We treat the personal information you provide to us as confidential and take reasonable steps, including standard industry safeguards to protection [sic] your personal information from accident deletion or loss and unauthorized access, disclosure or modification."); Global Privacy Statement, United States and Canada, Updated May 21, 2015, https://web.archive.org/web/20160204031954/http:/www.marriott.com/about/privacy.mi, last accessed Dec. 7, 2018 (same); Marriott Group Global Privacy Statement, Updated July 1, 2016, https://web.archive.org/web/20170218023855/http:/www.marriott.com/about/privacy.mi, last accessed Dec. 7, 2018 ("We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization.").

delete, or restrict the use of [his or her] Personal Data," Marriott states it "may need to verify your identity before fulfilling your request."

29. *Fourth*, the Global Privacy Statement indicates that it undertakes security measures and uses customers' data to do so. It states: "We use the data [from cookies] for security purposes[.]" It also states: "We use Personal Data and Other Data for certain analysis, audits, security and fraud monitoring and prevention[.]"

30. The data breach, even if just to the extent of the breach so far acknowledged by Marriott, shows that Marriott failed to fulfill the promises it expressly made in its Global Privacy Statement.

C. <u>The information in the Reservation Database is highly valuable.</u>

31. Marriott was or should have been aware that it was collecting highly valuable data, which the Federal Trade Commission describes as "good as gold" to criminals.[18]

32. Marriott itself uses personal information to profit through customized marketing (or as Marriott puts it, "We use Personal Data and Other Data to personalize the Services and improve your experiences"),[19] its loyalty programs, communications with customers, and the broadly defined category of "Business Purposes."[20]

33. The information in the Reservation Database is particularly valuable to hackers because it includes biographical data about its guests and "[i]ncreasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[21] Thieves can also use large pools of data, such as the Reservation Database to commit "synthetic identity

---

[18] Fighting Back Against Identity Theft, FTC Toolkit, http://www.browardcrime.org/images/CrimeCommissionBCCCKitidt06.pdf, at 21.
[19] Marriott Group Global Privacy Statement, Last Updated: May 18, 2018, https://www.marriott.com/about/privacy.mi.
[20] *Id.*
[21] Verizon 2014 PCI Compliance Report, http://www.verizonenterprise.com/resources/reports/rp_pci-report-2014_en_xg.pdf, at 54.

theft," which occurs when thieves combine information "into the equivalent of a bionic person. . . . the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number."[22]

34. Marriott knew or should have known that it had an obligation to secure the Reservation Database because it contains highly valuable information.

D. Marriott and the hotel industry have a history of being hacked.

35. Marriott and its competitors in the hotel industry are no strangers to being hacked.

36. Specifically, in 2015, Starwood, before it was acquired by Marriott, became aware of a malware intrusion that affected some point-of-sale systems in some Starwood hotels in North America. The infection of malware enabled "unauthorized parties to access payment card data of some of [Starwood's] customers."[23] In a November 2015 letter, Sergio Rivera, Starwood's President, notified consumers of the malware infection and stated that the company would, through AllClear ID, offer identity protection and credit monitoring services to affected customers for free for one year.[24] In January 2016, the Company sent a second letter listing the 106 affected hotels and the dates when the malware got into the point-of-sale system.[25]

---

[22] Pamela Yip, *Money Talk: Synthetic Identity Theft causing big headaches*, DALLAS NEWS, Aug. 2014, https://www.dallasnews.com/business/business/2014/08/31/money-talk-synthetic-identity-theft-causing-big-headaches (last accessed Dec. 7, 2018).

[23] Starwood Hotels and Resorts, Letter from our President, Nov. 20, 2015, https://www.starwoodhotels.com/Media/PDF/Corporate/Letter_1.pdf (last accessed Dec. 7, 2018).

[24] *Id.*

[25] Starwood Hotel and Resorts, Update Jan. 22, 2016, https://www.starwoodhotels.com/Media/PDF/Corporate/Hotel_List.pdf (last accessed Dec. 7, 2018).

37. As experts have noted, a "more thorough investigation into the 2015 investigation could have uncovered the [current] attackers, who instead were able to lurk in [Marriott's] reservation system for three more years."[26]

38. In June 2017, independent cybersecurity researchers detected another infection. According to *Forbes*, Marriott's Computer Incident Response team was compromised due to a mistake of a contracted cybersecurity vendor.[27]

39. Alex Holden, the founder of Hold Security, also sent *Forbes* screenshots that indicated cybercriminal access to Starwood corporate portals. Holden said that the images indicated a control panel used by "Russian criminals to run a network of hacked servers," Holden stated that "we know that they have access to infected computers that seem to access Starwood employee data and company resources."[28]

40. Holden detailed two additional and glaring security weaknesses from Marriott. He noted that there was an "easily guessable" password for Starwood's ServiceNow cloud computing service which could be used to access businesses' financial records, IT security controls, and bookings information.[29]

41. Holden also stated that there was a serious vulnerability on Starwood's website dating back to 2014. This "SQL injection bug" could have been exploited to gain access to

---

[26] Robert McMillan, *Marriott's Starwood should have detected hack years earlier, experts say*, MARKETWATCH, Dec. 2, 2018, https://www.marketwatch.com/story/marriotts-starwood-should-have-detected-hack-years-earlier-experts-say-2018-12-02 (last accessed Dec. 7, 2018).
[27] Thomas Brewster, Revealed: Marriott's 500 Million Hack Came After A String of Security Breaches, Dec. 3, 2018, https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#3dba0b9546f4 (last accessed Dec. 7, 2018).
[28] *Id.*
[29] *Id.*

Starwood databases. In fact, hackers on the dark Web dating back to 2014—the year of the data breach in this case—were offering to hack Starwood given these known vulnerabilities.[30]

42. Additionally, several of Marriott's competitors have been hacked in recent years. Specifically:

- In 2008 and 2009, hackers attacked Wyndham Worldwide Corporation and accessed more than 619,000 accounts. In 2015, the FTC and Wyndham settled with the FTC requiring Wyndham to undertake substantial monitoring for 20 years;[31]
- Between 2014-2017, Trump Hotels revealed three data breaches against the hotel;[32]
- On October 31, 2017, Hilton Hotels agreed to pay $700,000 to settle investigations by the New York and Vermont Attorneys General into two data breaches that exposed 363,000 credit card numbers;[33] and
- On March 17, 2015, the Mandarin Oriental announced that its credit card systems had been accessed without authorization as a "direct result of an unauthorized cyber-attack."[34]

---

[30] *Id.*

[31] Sean O'Neill, *Marriott's Starwood Data Breach Joins a Decade-Long List of Hotel Data Exposures*, SKIFT, Nov. 30, 2018, https://skift.com/2018/11/30/marriotts-starwood-data-breach-joins-a-decade-long-list-of-hotel-data-exposures/ (last accessed Dec. 7, 2018).

[32] *Trump hotels hit by third data breach*, BBC, July 13, 2017, https://www.bbc.com/news/technology-40593943 (last accessed Dec. 7, 2018).

[33] Jonathan Stempel, *Hilton to pay $700,000 over credit card data breaches*, REUTERS, Oct. 31, 2017, https://www.reuters.com/article/us-hilton-wrldwide-settlement/hilton-to-pay-700000-over-credit-card-data-breaches-idUSKBN1D02L3 (last accessed Dec. 7, 2018).

[34] Mandarin Oriental, *Statement Relating to Credit Card Breach Update – 17th March 2015*, Mar. 17, 2015 https://www.mandarinoriental.com/media/press-releases/statement-relating-to-credit-card-breach.aspx (last accessed Dec. 7, 2018).

43. In light of these numerous and repeated hacks, Marriott was on notice that it was a likely target for continued hacking and should have exercised particular care and vigilance with respect to its guests' PII. It failed to do so.

E. Marriott has harmed guests by allowing hackers to access their information.

44. Marriott caused harm to its guests by failing to prevent hackers from stealing their information. Whether or not their information is subsequently used in a criminal enterprise, the mere theft of PII significantly increases the risk of a guest's identity being exploited in ways that would cause economic harm, thereby decreasing the value of their PII, and requiring reasonable efforts to mitigate against that risk.

45. Plaintiffs and Class Members have a significant, imminent risk of identity theft because of Marriott's actions. Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration date, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[35] In some data breaches, as many as "1 in 4 . . . [eventually] became a victim of identity fraud."[36]

46. Identity thieves can use information from the Reservation Database to perpetrate a variety of crimes that harm Marriott's guests, including immigration fraud; obtaining a driver's license or identification card in the victim's name but with another picture; using the victim's

[35] FTC Consumer Information, Warning Signs of Identity Theft, http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last accessed Dec. 7, 2018).
[36] Al Pascual, 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, Feb. 20, 2013, javelinstrategy.com/brochure/276 (last accessed Dec. 7, 2018).

information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

47. Importantly, reimbursing a consumer for a financial loss due to fraud does not make that individual economically whole. This is so because "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[37] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[38]

F. Marriott's (belated) response is insufficient to mitigate Class Members' damages.

48. On September 8, 2018, Marriott stated that it received an alert regarding an attempt to access the Reservation Database.[39]

49. On November 19, 2018, Marriott claimed that it was able to decrypt the information that had been copied and encrypted and determined that the contents were from the Reservation Database.[40]

50. From there, Marriott waited an additional 11 days to inform the public of the data breach.

51. On November 30, 2019, in the wake of the data breach, Marriott created a website and call center, ostensibly to handle inquiries from its customers. Marriott has not, however, confirmed definitively which of its customers are affected nor attempted to meaningfully remediate its guests' losses. In particular, Marriott appears to offer two programs, both of which are at best cosmetic:

---

[37] United States Department of Justice, Bureau of Justice Statistics, Victims of Identity Theft, 2012, http://www.bjs.gov/content/pub/pdf/vit12.pdf, at 1 (last accessed Dec. 7, 2018).
[38] *Id.* at 11.
[39] Starwood Guest Reservation Database Security Incident, Nov. 30, 2018, https://answers.kroll.com/.
[40] *Id.*

a. Marriott offers guests who live in the United States, Canada, or United Kingdom one year of a program called WebWatcher, which ostensibly "keeps an eye on internet sites where thieves swap and sell personal information and then alerts people if anyone is selling their information."[41] There are three serious issues here. *First*, criminal activity following data breaches generally occurs on what is known as the Deep Web, which is hundreds of times larger than the "public" internet that one can search with services such as Google.[42] No program can truly monitor the entire Deep Web. *Second*, one year of WebWatcher protection is woefully insufficient for identity protection given that thieves can easily wait until such programs expire to use stolen data.[43] This is especially so since Marriott has publicly announced the expiration date of its protection. *Finally*, Marriott does not appear to be meaningfully publicizing even this meager step, meaning that the vast majority of eligible guests likely do not know that they are eligible.

b. Marriott announced that it will apparently pay to replace passports *after* guests prove that they have been victimized by passport-related identity

[41] Nicole Perlroth, et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES, Nov. 30, 2018, https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.
[42] Mae Rice, *The Deep Web is the 99% of the Internet You Can't Google*, May 22, 2018, https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-cant-google-curiosity/ (last accessed Dec. 7, 2018).
[43] Matt Tatham, *A Year After the Equifax Breach: Are You Protecting Your Data?*, Sept. 24, 2018, https://www.experian.com/blogs/ask-experian/a-year-after-the-equifax-breach-are-you-protecting-your-data/ (last accessed Dec. 7, 2018).

> fraud.[44] This seriously misses the point. Class Members whose passport information was stolen should get new passports *now*, not wait to see if a criminal happens to use their passport fraudulently. This is particularly so because of the very serious ramifications associated with identity theft involving one's passport; e.g., if a government were to flag one's passport number as suspicious or invalid.

52. Marriott further botched its own revelation of the data breach in two main ways: (1) it failed to send notice in a timely fashion to all affected consumers and (2) the form of the notice it sent was misleading.

53. To the first point, Marriott said that the process of emailing affected consumers will take weeks. This is far too long to communicate this critical information to consumers.[45]

54. To the second point, the email that Marriott sent to affected consumers came from "email-marriott.com." As technology reporters stated, "there was little else to suggest the email was at all legitimate—the domain doesn't load or have an identifying HTTPS certificate. In fact, there's no easy way to check that the domain is real, except a buried note on Marriott's data breach notification site that confirms the domain is legitimate."[46] Sending notice through a domain in this manner further subjected Marriott consumers to risk. To protect Marriott consumers, two different security experts had to register similarly named domains—email-

---

[44] Grace Dobush, *Starwood Data Hack: Marriott Says It'll Pay for New Passports*, Dec. 4, 2018, http://fortune.com/2018/12/04/starwood-hack-marriott-new-passports/ (last accessed Dec. 7, 2018).

[45] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WSJ, Dec. 2, 2018, https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

[46] Zach Whittaker, *Marriott's breach response is so bad, security experts are filling in the gaps—at their own expense*, TechCrunch, Dec. 3, 2018, https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/ (last accessed Dec. 7, 2018).

mariott.com and email-marriot.com—to protect consumers from clicking on an incorrect link.[47] Put bluntly, Marriott was unable to even send an email to its customers without creating a risk that customers' PII would be pilfered.

55. Marriott's untimely and inadequate response to the data breach does not change the fact that Marriott's conduct leading up to the breach directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII and PCD, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including the:

a. theft of their personal and financial information;

b. imminent and certainly impending injury flowing from potential fraud and identify theft posed by their passport, credit and debit cards, and personal information being placed in the hands of criminals;

c. untimely and inadequate notification of the data breach;

d. improper disclosure of their PII;

e. loss of privacy;

f. out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

g. deprivation of the value of their PII and PCD, for which there is a well-established market; and

h. overpayments to Marriott for products and services purchased during the data breach because the market price for Marriott's products and services would have been lower had consumers known of Marriott's inadequate security.

[47] *Id.*

56. Marriott also continues to maintain Class Members' information, apparently in the same insecure database from which it was stolen in the first instance. Plaintiffs and the Class have an immediate interest in ensuring that this information is secure and remains that way.

CLASS ACTION ALLEGATIONS

57. Plaintiffs bring this action on behalf of a class of:

> All individuals whose personally identifiable information and/or payment card data were in the Reservation Database at any time between January 1, 2014 and September 10, 2018.

To the extent necessary for manageability at trial, Plaintiffs propose that the Court certify state subclasses in order to group similar causes of action for states requiring similar evidentiary proof. Plaintiffs reserve the right to propose these or other subclasses prior to trial.

58. Excluded from the Class and any subclasses are Defendant, and its parents, subsidiaries, agents, officers, and directors. Also excluded is any judicial officer assigned to this case and members of his or her staff.

59. Plaintiffs seek class certification under Rule 23(b)(2) and Rule 23(b)(3) of the Federal Rules of Civil Procedure. In the alterative, they seek class certification under Rule 23(c)(4) because the below common questions predominate as to particular issues that could substantially advance the litigation. The Class meets all express and implied requirements of these rules.

60. **Ascertainability.** The Class is readily ascertainable because it is objectively defined and meets the ascertainability standard of this Circuit. Indeed, the Class consists of individuals whose information appears in Marriott's own database and thus meets the ascertainability standard of every Circuit.

61. **Numerosity—Rule 23(a)(1)**. Marriott admits that the personal information of hundreds of millions of guests has been compromised. Accordingly, the members of the Class are so numerous that joinder of all members is impracticable.

62. **Commonality—Rule 23(a)(2)**. The answer to at least one question common to the Class will drive the resolution of this litigation. For example:

a. Whether Marriott had a duty to take reasonable and prudent security measures.

b. Whether Marriott failed to take reasonable and prudent security measures.

c. Whether Marriott's failure to take reasonable and prudent security measures caused injury.

d. Whether Marriott disclosed Plaintiffs' and Class Members' PII without their consent.

e. Whether Marriott violated Maryland law when it failed to implement reasonable security procedures and practices.

f. Which security procedures and which data-breach notification procedure Marriott should be required to implement.

g. Whether Marriott has a contractual obligation to use reasonable security measures.

h. Whether Marriott has complied with any contractual obligation to use reasonable security measures.

i. What security measures, if any, must be implemented by Marriott to comply with its contractual obligations.

j. Whether Marriott violated state privacy laws in connection with the actions described herein; and

k. Whether Plaintiffs and Class Members are entitled to damages, declaratory, or injunctive relief.

63. **Typicality—Rule 23(a)(3).** Plaintiffs bring claims for the same type of injury under the same legal theory as the rest of the Class. Among other things, Marriott exposed all Class Members' personal information through the same database.

64. **Adequacy—Rule 23(a)(4)**. Plaintiffs and their counsel are adequate because: (1) there no conflict between the proposed Class representative and other Class members, or, to the extent any conflicts develop, undersigned counsel will propose the appointment of interim class counsel to represent the various Class members' interests; and (2) the proposed Class representatives and their counsel will vigorously pursue the claims of the Class. Plaintiffs have no interests contrary to, or in conflict with, the interests of Class Members.

65. **Predominance & Superiority—Rule 23(b)(3)**. Common issues in this litigation predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. A class action, moreover, is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

66. **Final injunctive relief is appropriate respecting the Class as a whole—Rule 23(b)(2).** Injunctive relief is appropriate because, among other reasons, Marriott's inadequate security exposes all Class Members to a substantial risk of immediate harm. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence

67. Plaintiffs incorporate the above allegations as if fully set forth herein.

68. Marriott knew or should have known that its database and data repositories were vulnerable to unauthorized access by third parties.

69. Marriott assumed a duty of care to use reasonable means to implement both a policy and process by which it could prevent such unauthorized access. Further, Marriott was responsible for engaging in supervision, monitoring and oversight consistent with the PII that was collected, used, and shared by it.

70. Marriott owed a duty of care to Plaintiffs because it stored Plaintiffs' and the Class Members' PII and they were foreseeable and probable victims of any inadequate security related policies and practices. Marriott had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of the Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Marriott did not protect Plaintiffs' and Class Members' information from hackers.

71. Marriott's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Marriott's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

72. Marriott acknowledged the importance of keeping this information secure, and stated that they sought "to use reasonable organizational, technical and administrative measures to protect Personal Data." Despite acknowledging their responsibility to keep this information secure, Marriott improperly put the burden on Plaintiffs and Class Members to notify Marriott if they suspected that their information was not secure, when individuals would not have access to this information, and Marriott was in a superior position to know this information, and were in the exclusive possession of such information.

73. Upon information and belief, Marriott improperly and inadequately safeguarded the personal and confidential information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the data breach.

74. Marriott's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive personal and confidential information has caused Plaintiffs and Class Members to suffer injury and damages. As described herein, Plaintiffs now must take and have taken affirmative steps to ensure that their identity is not stolen and their financial information is not compromised.

75. Marriott breached these duties in failing to take reasonable measures or to implement reasonable policies and procedures to prevent the unauthorized access to the PII of Plaintiffs.

76. Marriott further breached these duties in failing to take reasonable measures or to implement reasonable policies and procedures to detect an intrusion into their Reservation Database.

77. Marriott further breached these duties in failing to take reasonable measures or to implement reasonable policies and procedures to notify Plaintiffs and Class Members of the data breach.

78. As a result of the breach, Plaintiffs suffered damages, and the damages available by way of contract remedies would be inadequate to fully compensate them for their losses.

SECOND CAUSE OF ACTION
Breach Of Contract

79. Plaintiffs incorporate the above allegations as if fully set forth herein.

80. Marriot expressly promised to Plaintiffs and Class Members, through its publication of its Global Privacy Statement, that it would safeguard Plaintiffs' and Class Members' PII and PCD. In exchange for that and other promises made by Marriott, Plaintiffs and Class Members agreed to the purchase and use of Marriott's hotel services.

81. The Global Privacy Statement indicates that Marriott agreed to properly maintain Plaintiffs' and Class Members' PII and PCD, enact safeguards to protect the data, and limit access to PII and PCD.

82. Marriott breached its promises by failing to safeguard Plaintiffs' and Class Members' PII and PCD, failing to detect the data breach, and failing to notify Plaintiffs and Class Members in a timely fashion of the data breach.

83. Plaintiffs and Class Members have performed all, or substantially all, of the obligations imposed on them under the Global Privacy Statements.

84. Plaintiffs and Class Members have been damaged as a result of Marriott's breach of its promises.

THIRD CAUSE OF ACTION
Breach of Implied Contract

85. Plaintiffs incorporate the above allegations as if fully set forth herein.

86. Alternatively, if Marriott's express promises made in its Global Privacy Statement do not obligate it to protect Plaintiffs' and Class Members' information and to timely and accurately notify Plaintiffs and Class Members if their data had been breached or compromised,

then Plaintiffs alleges that there exists an implied contract whereby Marriott is obligated by the covenant of good faith and fair dealing, to meet those same obligations.

87. If the Court determines that Plaintiffs cannot bring a cause of action for breach of contract, Plaintiffs assert a cause of action for the breach of the covenant of good faith and fair dealing.

88. Marriott's Global Privacy Statement contained the implied promise that it would safeguard and limit disclosures of customers' PII and PCD. The Global Privacy Statement contained clear information about the limited uses of PII and PCD. Further, it mentioned the security efforts that Marriott had in place to protect data.

89. On this basis, Marriott informed Plaintiffs and Class Members that providing their PII and PCD would be safe. Plaintiffs and Class Members accepted these offers made by Marriott in allowing Marriott to store, maintain, and safeguard their personal and confidential information.

90. When Plaintiffs and Class Members provided their personal and confidential information to Marriott in connection with staying in a Starwood Property, they entered into implied contracts with the Marriott, pursuant to which Marriott agreed to safeguard and protect their information, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached or compromised.

91. Plaintiffs and Class Members would not have provided to and entrusted their personal and confidential information with Marriott in connection with staying in a Starwood Property in the absence of the implied contract between them.

92. Plaintiffs and Class Members fully performed their obligations under the implied contract with Marriott.

93. Marriott breached the implied contract it made with Plaintiffs and Class Members by failing to safeguard and protect the personal and confidential information of Plaintiffs and Class Members and by failing to provide timely and accurate notice to them that their information was compromised in and as a result of the data breach.

94. As a direct and proximate result of Marriott's breaches of the implied contracts between Marriott and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

FOURTH CAUSE OF ACTION
Violation Of The Maryland Consumer Protection Act,
Md. Comm. Code §§ 13-301, *et seq*.

95. Plaintiffs incorporate the above allegations as if fully set forth herein.

96. Marriott is a "person" as defined by Md. Comm. Code § 13-101(h).

97. Marriott's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

98. Plaintiffs and Class Members are "consumers" as defined by Md. Comm. Code § 13-101(c).

99. Marriott advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d)(2).

100. Marriott engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Failing to state a material fact where the failure deceives or tends to deceive;

c. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

d. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

101. Marriott engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' personal and confidential information, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal and confidential information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' personal and confidential information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

102. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect consumers' PII. Marriott's misrepresentations and omissions would have been important to a significant number of consumers in making decisions related to financial transactions with Marriott.

103. Marriott intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

104. Had Marriott disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been forced to adopt reasonable data security measures and comply with the law.

105. Marriott acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class Members' rights. Marriott was on notice of the possibility of the data breach due to its prior data breach and infiltrations of its systems in the past as well as infiltrations of other hotel chains.

106. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PCD.

FIFTH CAUSE OF ACTION
Declaratory Relief

107. Plaintiffs incorporate by reference all factual allegations as if fully set forth herein.

108. There is an actual controversy between Marriott and Class Members concerning whether Marriott has a duty to implement additional safeguards to protect the PII of Plaintiffs and Class Members.

109. Pursuant to 28 U.S.C. § 2201, this Court may "declare the rights and legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought."

110. Accordingly, Plaintiffs and Class Members seek a declaration that Marriott has a duty to implement safeguards to guard against the future exposure of Plaintiffs' and Class Members' PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. Certify this case as a class action, appoint Plaintiffs as Class representatives, and appoint Plaintiffs' counsel to represent the Class;

b. Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages;

c. Award equitable, injunctive, and declaratory relief as may be appropriate, including without limitation an injunction;

d. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

e. Award pre-judgment and post-judgment interest as prescribed by law; and

f. Grant further and additional relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: December 7, 2018

Respectfully submitted,

/s/ Cary Joshi

Benjamin L. Bailey*
John Roddy*
Michael L. Murphy*
Cary Joshi (D. Md. #20621)
Bailey & Glasser LLP
1054 31st Street, NW Suite 230
Washington DC 20007
Telephone: 202-436-2101
Fax: 202-463-2103
BBailey@baileyglasser.com
JRoddy@baileyglasser.com
MMurphy@baileyglasser.com
CJoshi@baileyglasser.com

Michael W. Sobol*
David T. Rudolph*
LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
msobol@lchb.com
drudolph@lchb.com

Jason L. Lichtman*
Sean A Petterson*
LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212.355.9500
jlichtman@lchb.com
spetterson@lchb.com

Attorneys for Plaintiffs and the Proposed Class

**Pro hac vice* applications forthcoming